



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/537,068	03/28/2000	Ronald P. Doyle	RSW9-2000-0002-US1	5371

7590 05/26/2006

Jeanine S Ray-Yarletts
IBM Corporation 972/B656
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER

WRIGHT, NORMAN M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/537,068
Filing Date: March 28, 2000
Appellant(s): DOYLE, RONALD P.

Marcia L. Doubet
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/17/2006 appealing from the Office action mailed 07/25/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. However, the changes are as follows: Appellant has included arguments that the After Final Amendment should have been entered. This issue is not appealable, it is a petitionable issue. Accordingly it has been rendered as moot for the purpose of this answer, and will not be treated further by the examiner.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6510236	Crane et al.	1-2003
6016476	Maes et al.	1-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4,7,10-13 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Crane et al., U.S. Patent Number 6,510,236, hereinafter '236.

Claims 5-6,8-9,14-15, and 17-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane '236 as applied to claims 1-4,7,10-13 and 16 above, and further in view of Maes et al., U.S. Patent Number 6,016,476, hereinafter '476.

The final office action has been reproduced below for your convenience:

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-4, 7,16, 10-13, are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Crane et al., U.S. Pat. No. 6,510,236 B1, hereinafter '236.

As to claims 1-4, 7, 16 and 10-13, '236 teaches the claimed invention of an authentication framework for managing authentication request comprising: a compute program product for use with biometrics, a pervasive device, capturing biometric data, a first or second party/user, a reader, means for identifying by comparing stored data, capturing biometric data, transmitting, retrieving, and returning information/authentication token, access rights/tokens, locally stored data, and a photograph {biometrics, picture/scan of finger, palm, eye etc}, and a remote server, a trusted application server, (abs., figs. 1-4, col. 1, lines 45 et seq., col. 2, lines 20 et seq., col. 3, lines 8-13, 29-32, and 47-67, col. 4, lines 25 et seq., col. 5, lines 1-40, claim 23, col. 6, line 25 et seq.).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 5-6, 14-15, 8-9, 17-18, and 19-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over '236 as applied to claims 1-4, 7, 16, and 10-13 above, and further in view of Maes et al., U.S. Pat. No. 6,016,476, hereinafter '476.

5. As to claim 5-6, and 14-15, '236 do not explicitly teach the retrieval of information from a protected non-locally accessible data means, or filtered data. '476 teaches filtering and, non-locally accessible data (abs., figs. 1 and 5-6, col. 1, lines 14 et seq.,

Art Unit: 2134

col. 2, lines 24 et seq., col. 3, col. 5, lines 25 et seq., and col. 7, lines 5 et seq.) It would have been obvious to one of ordinary skill in the art at the time of the invention, to augment the invention of '236 with a means providing a portable information and transaction system utilizing biometrics as disclosed in '476. One of ordinary skill in the art would realized the advantages of not providing any additional information that may not be locally accessible on the pervasive device, within a transaction system. One of ordinary skill in the art would have been motivated to perform such a modification, because, one of ordinary skill would have had a desire not to transmit any additional personal authentication information to a device that did not possess it, as a means of safeguarding the confidentiality and integrity of one's personal data. With such a desire in mind one could not only safeguard information that a device is not purvey to, but, stop the erroneous transfer of another personal information (col. 7, lines 5-10 et seq.). '476 also recites that it may be used in a security system to access applications and systems for a device or building (col. 2, lines 50-60 et seq.), therefore, it would lend itself well to the uses described in the invention of '236.

6. As to claims 8-9, and 17-18, '236 does not explicitly teach the transmission of a trusted message or a secure meeting where the coded means is used to identify attendees at a meeting. '467 teach the use of transmitting trusted messages (col. 2, lines 23-67 et seq., col. 3, lines 15-35 et seq., and 40-67 et seq.) and, providing access to a secure building via the use of a pervasive device or code (col. 2, lines 50-58).

7. As to claims 19-27, they recite a concomitant of previously recited elements and therefore fail to distinguish over the above rejected claims, accordingly, they are rejected under the same rationale, see above.

Response to Arguments

Applicant's arguments filed 12/6/04 have been fully considered but they are not persuasive. The distinction between party, users, clients and device users is not understood. The possessor of a device /party may use his device to authenticate another party/device/client/user which maybe broadly interpreted as parties. Party maybe broadly construed as a group or individual participating in an activity, therefore, clients, users and devices user would all classify as parties.

(10) Response to Argument

In response to appellant's argument that the reference Crane '236 fails to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., **first and second parties are simultaneously...**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. In fact the claims fail to recite any mentioning of gathering or causing a first party's biometric to be captured, identified or verified. Moreover, the specification does not appear to have said limitation contained within it. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In particular claims 1 and 10 does not in fact recite or inherently possess the feature described in appellant's argument. Claim 1, does recite that a computer program product has embodied thereon code for: "... [causing] means for identifying said second party..." Therefore, it is clearly understood that the program product does not impart simultaneous operations to the biometric device for multiple simultaneous users. Because, the disclosure as indicated by appellant, at 12, line 9-13, only sets forth the validation, privilege determinations, or identity processing as required by an application. A plain reading of the specification and claim 1, fails to convey any embodiment or fore knowledge of a system that is simultaneously processing the captured biometric data of two different entities.

Claim 10, which recites the system elements of the claimed invention, contemplates a device that is possessed by a first party and has means for capturing biometrics of a second party. Appellant has made a number of remarks regarding possess. As understood by the examiner, posses in its simplest definition means to own or have ownership of, or to have as property, it may even mean to have, hold or seize. None of these definition imparts the simultaneous uses of a biometric as disclosed by applicant. It is not a feature of claims 1 or 10 and has not been contemplated as evidenced by the claims lacking a feature that corresponds to it. Moreover, claims 1 and 10 individually or collectively fails to recite any features that would inherently perform such a process as simultaneously processing biometric data of two different parties.

Notwithstanding, the term party allow for any individual, group, organization or entity to be the owner or holder of the device, is not a patentable distinction. In '236, the background goes into what types of networks and servers are commonplace today, they include private networks, corporate intranets, or the world-wide-web internet/ public networks (col. 1, lines 15-20 et seq.). It is in this environment that '236 contemplate the use of his invention for authenticating clients having a plurality of authentication devices (col. 1, lines 53-60 et seq.). Additionally, '236 utilize an authenticating framework for use in "authenticating clients having a plurality of ... devices [which maybe similar or different, '236 col. 1, lines 61-67 and col. 2, lines 1-5 et seq.]." Therefore, the clients, corporations, users, or other intra- or internet entities own and therefore possess their authenticating devices.

The fact that a person may have ownership or physical possession of a device would not in and of itself, be a patentable distinction. The system put forth by appellant is devoid of any element or structure that make the authentication system of appellant materially and patentably different for the prior art systems. In-fact, appellants' own drawing (figs. 1 and 2) show that appellant's system is nothing more than the **prior art**. It also has at its core the very same 3 elements of processing biometrics as '236, namely a client authentication device (10, 300, 310), an application server (42, 44, 46 and 325) and authenticating server (47 and 335/340) see figure 3. The description of appellant specification, discloses that the environment is the same (pg. 8, description of preferred embodiment). Then at page 12, second paragraph, appellant describes that his biometric device is one "which is commercially available to attach (or may be

Art Unit: 2134

incorporated within the pervasive device. Page 2, of the first paragraph of appellant disclosure gives examples of current and prior art pervasive devices, for “[example] devices include cell phones..., computing devices..., devices adapted for use in home or vehicles..., mobile computers, PDAs, handheld computers ... PalmPilot.” On page 4 of his disclosure, he gives prior art examples of pervasive devices (according to his examples recited above) utilizing biometrics and photographic images for identification and verification. Stated differently his prior art utilizes pervasive devices and computing devices of the prior art, to perform existing techniques to identify, verify and/or authenticate entities based upon biometrics. These are believed to be clear reasons showing why the present invention fails to distinguish over the prior art.

Notwithstanding, there appears to be a complete failure of appellant to disclose a simultaneous action involve when capturing biometrics as argued by appellant, it does not appear in the claims or the specification.

MPEP 2112.01 [R-3]

Composition, Product, and Apparatus Claims

I. PRODUCT AND APPARATUS CLAIMS — WHEN THE STRUCTURE RECITED IN THE REFERENCE IS SUBSTANTIALLY IDENTICAL TO THAT OF THE CLAIMS, CLAIMED PROPERTIES OR FUNCTIONS ARE PRESUMED TO BE INHERENT

Where the claimed and prior art products are identical or substantially identical in structure or composition, or are produced by identical or substantially identical processes, a prima facie case of either anticipation or obviousness has been established.

In re Best, 562 F.2d 1252, 1255, 195 USPQ 430, 433 (CCPA 1977). “When the PTO shows a sound basis for believing that the products of the applicant and the prior art are the same, the applicant has the burden of showing that they are not.” In re Spada, 911 F.2d 705, 709, 15 USPQ2d 1655, 1658 (Fed. Cir. 1990). Therefore, the prima facie case can be rebutted by evidence showing that the prior art products do not necessarily possess the characteristics of the claimed product. In re Best, 562 F.2d at

Art Unit: 2134

1255, 195 USPQ at 433. See also *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985)

As to the fact that prima facie obviousness has not been established for claims 1-4, 7, 10-13 and 16, the examiner does not concur. Appellant has failed to demonstrate any patentable distinction for his apparatus, method, or program product, instead he has generalized to say that all elements have not been identified. He has identified two aspects that he considers to be different: namely a first party possessing (the biometric device) and a second party (the user of the device to be authenticated). Appellant's device and system apparently has no structural differences for the prior art, as evidenced by Appellant's drawings figures 1-2, and his specification, on pages 11-12 he utilizes well known software, hardware and networks as is commonly known to one of ordinary skill in the art. Appellant states, "the user device may be any kind of pervasive device having processing and communication capabilities.... The server can be one of any...processing and communication capabilities. These techniques are well known in the art, and the hardware devices and software, which enable their use are readily available." Recalling that, on page 4 of his disclosure, he gives prior art examples of pervasive devices utilizing biometrics and photographic images for identification and verification. Stated differently his prior art utilizes pervasive devices and computing devices of the prior art, to perform existing techniques to identify, verify and/or authenticate entities based upon biometrics. He now asserts that his operation is different because a first party possesses the device. The possession of this device is not integral to its function and operation. It still requires the biometric sample from a user, a database upon which to match a person's template and communication to convey said

Art Unit: 2134

information. The user is authenticated in the same manner that biometric devices conventionally verify people identities. Without getting into or even arguing the definition of posses, the use of a device can not serve to distinguish a system, apparatus or product, if there is no structural differences.

2114 [R-1]

Apparatus and Article Claims — Functional Language

For a discussion of case law which provides guidance in interpreting the functional portion of means-plus-function limitations see MPEP § 2181 - § 2186.

APPARATUS CLAIMS MUST BE STRUCTUR-ALLY DISTINGUISHABLE FROM THE PRIOR ART

>While features of an apparatus may be recited either structurally or functionally, claims<directed to >an< apparatus must be distinguished from the prior art in terms of structure rather than function. >In re Schreiber, 128 F.3d 1473, 1477-78, 44 USPQ2d 1429, 1431-32 (Fed. Cir. 1997) (The absence of a disclosure in a prior art reference relating to function did not defeat the Board's finding of anticipation of claimed apparatus because the limitations at issue were found to be inherent in the prior art reference); see also In re Swinehart, 439 F.2d 210, 212-13, 169 USPQ 226, 228-29 (CCPA 1971);< In re Danly, 263 F.2d 844, 847, 120 USPQ 528, 531 (CCPA 1959). "[A]pparatus claims cover what a device is, not what a device does." Hewlett-Packard Co. v. Bausch & Lomb Inc., 909 F.2d 1464, 1469, 15 USPQ2d 1525, 1528 (Fed. Cir. 1990) (emphasis in original).

MANNER OF OPERATING THE DEVICE DOES NOT DIFFERENTIATE APPARATUS CLAIM FROM THE PRIOR ART

A claim containing a "recitation with respect to the manner in which a claimed apparatus is intended to be employed does not differentiate the claimed apparatus from a prior art apparatus" if the prior art apparatus teaches all the structural limitations of the claim. Ex parte Masham, 2 USPQ2d 1647 (Bd. Pat. App. & Inter. 1987) (The preamble of claim 1 recited that the apparatus was "for mixing flowing developer material" and the body of the claim recited "means for mixing ..., said mixing means being stationary and completely submerged in the developer material". The claim was rejected over a reference which taught all the structural limitations of the claim for the intended use of mixing flowing developer. However, the mixer was only partially submerged in the developer material. The Board held that the amount of submersion is immaterial to the structure of the mixer and thus the claim was properly rejected

Appellant also asserts, that '236 fail to teach authenticating a user distinct from appellant's two party claim, in that it does not involve a technique involving a first and second party. **Claim 1 and 10, as presented requires that the device capture biometric data of a second party, only.** There is no recitation regarding the first party being authenticated, or having his data scanned or captured. Claim 1, recites "...capturing...biometric data of a second party...identifying a second party..." Claim 10, recites "capturing biometric data of a second party...identifying said second party..." Therefore, it is not relevant whether or not Crane '236 teach this feature, as it is not elements of the outstanding claims. Accordingly, the remarks regarding these features are moot.

Appellant also remarks that the un-entered amendment has certain recitations, these arguments are moot. The substance of an un-entered amendment is not substance for an appeal, it could have been petitioned. However, Appellant did not petition the un-entered amendment and does not have entry, as a matter of right to an un-entered after final amendments, see MPEP 714.13. Accordingly, the examiner will not discuss or address remarks related to this issue any further, within this answer.

The examiner has addressed the remarks put forth by appellant as to why the lacking of a different structure or elements, fails to distinguish appellant systems over the prior art, '234. The examiner has reminded appellant that the apparatus or device claims must distinguish over the prior art in terms of structural rather than function. Indeed, appellant invention utilizes the prior art to authenticate a second party/client who wishes to be verified or authenticated using biometrics. Crane '236, teach that

clients may be verified by the use of their biometrics on a pervasive device/16/token cards/generic devices (col. 3, lines 17 et seq. and col. 4, lines 24-34 et seq.). He recites that "one of ordinary skill will appreciate that the computer may also be a notebook, diskless computer..., or a pervasive computing device (PDA, smart phone etc.), at column 4, lines 23 et seq." He also states that the authentication device may utilize various pervasive and biometric devices to obtain the clients/second party data for verification.

As to the remarks of the first party being a possessor, i.e. having ownership of or hold of the device. The examiner finds that '236 teach the use of corporate networks, intranet networks, internet (private/public) networks and various clients, workstations, PDAs, laptops, mobile computers, smart phones etc utilize pervasive devices. These devices are under the ownership individuals, groups, organization, or corporations and these entities posses them. The clients of said entities allow or require the authentication of individuals, groups, clients and other entities/ second parties to verify their identity. Thus, the functional manner of operating a claimed apparatus or device regardless of who owns or holds the device does not serve to differentiate the claimed apparatus or product from the prior art.

Stated differently, the claimed limitations of a person being the possessor of a device, meaning either ownership or holding it, while another person is being authenticated is at the very least, nonfunctional descriptive language. Here, we see that the device would operate the same whether or not one person or another person held/owned it. The limitation of possession, which is a descriptive term does not relate

Art Unit: 2134

to nor does it affect the functionality and operations of the biometric pervasive device.

As a result, the functionally language does not limit the claim and thus not can not serve to distinguish.

As to the features of having simultaneous operations, and a two party technique for identification these remarks are moot. As having not been recited in the claims or disclosure of appellant's invention.

Appellant also remarks that the prior art fails to each and every feature of the claimed invention again, the examiner broadly construes the two parties as one who owns or holds the device upon which another (second party) is authenticated. The ownership or physical possession of the device, does not affect the operations of the biometric device, it does not change the structure, nor does it present new, non-obvious or novel functions that were not previously inherent to the device. It does provide a person with ownership (seller, merchant, corporation) possession of the device an ability to authenticate individuals (clients, buyers, users), who may use biometric data as a means of authentication. Appellant appears to have identified a difference in wording, not a patentable distinction.

Appellant also claims that the prior art fails to teach the use of a photograph as biometric data, as recited in claims 3 and 12. First, a brief review of biometrics and their operations will be given, which is consistent with the knowledge of one of ordinary skill in the art.

Generally, biometric technology involves the collection of data with a sensor. The sensing data is collected via a device, the data represents a digital format of

physiological features unique to an individual, such as facial imaging (infrared and optical), fingerprints and palm printing, patterns of the iris, the retina, veins, voice patterns, shape of the hand geometry, signature, keystroke etc. and also behavioral patterns. The collected biometric data may then be transformed, via an algorithm, to produce a digital image/photograph known as a template. This template or digital image is designed to be irreversible, meaning that a person can not deduce the biometric data from it. Templates are stored in a database that is accessed when an event occurs that is triggered by a biometric reading device, such as an authentication request. Some of the most common examples of biometric devices are scanners, touch pads/displays, cameras, microphones etc. Note, that it is the transmission of the original biometric template or image or digital photograph or data from said devices, such as fingerprint, hand, face, eye, voice, or behavior, is then sent to the network or system and retained for authentication. Following a similar algorithmic transformation of the second biometric template or image data, from an individual desiring to be authenticated, a comparison can be made. If a matching template or digital photographic image is found, of the person presenting the second biometric data, then the system or network recognizes and thus authenticates the individual. In short a biometric system is a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by a user as a digital template or image or photograph.

The use of photographs, biometric scanners, touch pads, or cameras, utilize facial, fingerprint and palm data, utilized as both static (photographic) and dynamic

Art Unit: 2134

(motion via camera) image data from the person who is to be authenticated, as well as other biometrics attributes, are notoriously well-known to persons of ordinary skill in the art. A person of ordinary skill in the art would have readily envisaged the use of photographs for biometric data collection, whether dynamic (camera) or static (picture/mug shots), would have been readily available for use in a biometric data authentication systems. Because, the biometric data collected from a scanner or pad or camera is readily converted to a digital template or image or photograph (collected sample) and that sample is compared to a stored data sample regardless of the input means used to collect it. Stated differently, the biometric data gathered is utilized to produce a digital photographic image of the persons' face, fingerprints, or palm etc, as is known in the art to as a template or digital image. The template is compared with the stored template or digital image to produce a desired authentication result. Regardless of the digital images' source, fingerprints are compared with fingerprints templates, facial digital images (pictures/static or camera/dynamic) with facial images templates, and palm digital images with palm images templates in the database. All of this is well known to a person of ordinary skill in the art.

Furthermore, as to Appellant's assertion regarding the use of photographs, the examiner in his office actions dated 3/25/04 and 6/1/04, recited the feature which he construed to be a photograph "{biometrics, picture/ scan of finger palm, eye etc.}," see '236 at col. 1, lines 40-45; where it states that clients have been provided with alternative means of authentication devices including biometrics, for example finger, eye or voice print, scanners convert the biometric data into a digital image or template. '236

Art Unit: 2134

at column 2, lines 1-5 and 18-25 states that it is the object of Crane '236 to provide a server with the capability of managing authentication request, from a variety of clients having disparate authentication devices and schemes. Photographs, voice prints, palm prints, fingerprints, eye scans etc., are a few of the various forms of biometric readers known to persons of ordinary skill in the art. On column 3 lines 29-30, '236 state that "authentication devices include, for example, token cards and biometric (e.g. finger, eye or voice prints) scanners." At column 4, lines 25-40, he describes the type of "computers, or a **pervasive computing device (e.g. a personal digital assistant, smart phone, or the like)**, upon which he invention will operate. Later he goes further to state, "In operation, the authentication device reads or otherwise obtains data appropriate for the method of authentication." Therefore a clear reading leads one to understand that his invention may be used on various biometric devices (input devices), which, are not limited to the finger, eye, or voiceprints disclosed in his system, nor is it limited to a single biometric characteristic. But that his desire is to provide a system that is adaptable to various authentication devices/schemes already in existence and upgradeable to future authentication devices and schemes, see column 6, lines 15-23. It is understood from '236 that the term 'biometric' encompasses other generally recognized devices that are not listed.

The examiner believes that the inventor of '236 intended for his invention to be incorporated into the well-known biometric devices at the time of his filing of the application. This point is made abundantly clear by the following: '236 in his background (col. 1, lines 47 et seq.) describes his view of the state of the prior art, he

states, **“Numerous third parties provide biometric scanning systems. A representative patent illustrating a biometric personal identification system based on iris analysis is U.S. Pat. No. 5,291,560, [hereinafter ‘560, patented March 1, 1994]. While these devices provide significant advantages, each authentication device has a different way of encoding input information and validating the user’s identity.”** The different input devices refers to the different type of biometric devices used to gather the biometric characteristic that is to be utilized for authentication. It is, the ‘560 patent with a date of 1994 reference, that ‘236 is referring back to, that has a disclosure describing the state of the art at that time. It is also the ‘560 reference, that is indicative of the breadth that the term biometrics encompasses. It is interesting to note that ‘560 of 1994, background recites a few of the well-known biometrics include, “signatures, **photographs**, fingerprints, voice prints and retinal,” column 1, lines 52-57 et seq. Looking at the fact that Daugman ‘560 was filed on July 15, 1991, one can reasonably conclude that the use of photographs as a biometric must have been well known at least by the 1991 filing date. This lead the examiner to believe that the Crane ‘236 reference filed on December 11, 1998, a full 2 years and 3 months prior to appellant’s application, and the Daugman ‘560 filed nearly 9 years before appellant’s invention, both recognized that the terms biometric is used for a broad range of security input devices and of various types. It is further understood, by those of ordinary skill in the art, that the term **biometric** is not to be limited to only a particular device and it is recognized in the art to represent a plurality of attributes not just those expressly recited as examples. In fact ‘560 recites that, “other biometrics such as signatures,

photographs, fingerprints, voice prints and retinal,” are known, and suggest that this is only exemplary of some of the biometrics used and not an all-inclusive list. 7 1/2 years later ‘236 Crane goes further to state that, “Numerous third parties provide biometric scanning systems. A representative patent illustrating a biometric personal identification system based on iris analysis is U.S. Pat. No. 5,291,560,” see ‘236 at col. 1, lines 47,” thereby explicitly stating that there are other biometric beyond the examples given. ‘236 further explicitly recite that the object of his invention is to provide a system that is adaptable to various authentication devices/biometric schemes already in existence and upgradeable to future authentication devices and schemes, see column 6, lines 15-23. Stated succinctly, neither the ‘560 or the ‘326 patents, filed respectively nearly 9 and 2 1/4 years before appellant’s application, meant for their examples of the operation of their biometric devices to be an all inclusive list. The inventor of Crane ‘236 has not given any indication that his invention is only useful in the examples depicting the limited biometric devices described in their respective patents as exemplary embodiments. Additionally, the use of photographs as a biometric was well known to persons of ordinary skill in the art, as early as 1991, as evidenced by above. Since, they knew that other biometric devices existed they gave examples of some of the more readily known devices. ‘236 in claim 6, speaks to the generality of a biometric scanner. While ‘560 gives a specific example using an iris scanner. Notwithstanding, the operations of biometric devices, routinely compares input template (digital photographic) data to stored data to determine authentication.

The point may be clarified further as disclosed by appellant's admission of what is well-known in the art. Appellant in his description of the related art, teaches the same pervasive devices (page 2, lines 1-0 et seq.); containing a similar overview of the general operations of biometrics (page 3, lines 6-14 et seq.); and two Fishbine et al. references (page 4, 2nd. Para.). These prior art references, filed on 11/19/91, and patented on 6/22/1993, U.S. Pat. No. 5,222,152, hereinafter '152, and Fishbine et al, filed on 3/31/1993, and patented on 11/14/1995, U.S. Pat. No. 5,467,403, hereinafter '403, both reciting the well known use of biometrics incorporating fingerprints, optical or photographic (mug shot), and optically mechanism to generate digital images for personal verification ('152 at col. 1, lines 40-60 et seq., col. 2, lines 10-20 et seq., claim 1). Furthermore Appellant's disclosure at page 5, lines 5 et seq., recite that the prior art, "The '152 and '403 patents use a portable device for capturing fingerprint data and photographic images," similar recitation is found on page 15 of appellant's disclosure. This admission of the prior art ('152 and '403) utilizing and performing the well known task of photographic processing of a biometric (also in '560) is now being asserted for the first time by appellant to be missing from the '236 reference. The two references clearly show that scanning may be used to gather biometrics images from fingerprinting as well as photographic images and to display a photograph, as recited in the '156 summary. Moreover, appellant's disclosure recites, "For example, when the retrieved information includes a picture of the person corresponding to the captured biometric data, ... preferably display the picture (page 14, 2nd. Para.)". This is the only mention of biometrics using a photograph or picture, all the other references to

Art Unit: 2134

photographs and pictures are made with reference to the prior art '152 and 403.

Therefore, it is not understood why, appellant now assert that the prior art fails to teach retrieved information comprising a photograph. It is the examiner's understanding, that retrieving a biometric photographic image, or biometric digital image, or a biometric template image (comprised of facial, fingerprint, palm, voice data etc.) is a representation of unique biometric characteristic of the person seeking to be authenticated, as is known in the art to persons of ordinary skill. Stated differently, it is the biometric template or digital data image or photograph that is store and represents the user as authenticating data, and thus, it is the matching of these templates that corresponds to each and every individual user. Computing devices do not transport photographic information, as humans see a picture, instead is it transports a digital representation of an image and process this image on the receiving end for viewing with the proper formatting that is needed on a display device. Again, it is the template image of the person that is retrieved and processed to produce a picture, as is known in the data processing arts.

Notwithstanding, the template image or retrieving of a photographic image for display has been taught as recited in '156, 204, '250, and even '236 as biometric data (i.e. templates image). Appellant's claims 3 and 12, at best appears to be retrieving photographic/template image data information, which would then indicative of an authentication result to a user device. The retrieving of said photographic information or data has been described in the prior art and lacks any novelty regarding its use in the instant invention. The retrieve photographic information is and should be construed as

Art Unit: 2134

a template of the second/party/user. The fact that appellant may desire to send a photograph or processed template, i.e. a template that has been processed through the algorithmic transform and interface program, to a user in a display has not been claimed. Claims 3 and 12, appears to have retrieved template data, which has been described or thought of as photographic data, which would be understood by a person of ordinary skill in the art. The photographic retrieved template does not appear to perform any new, novel, or non-obvious step, function, or provide and structural differences for a biometric template image as is known in the prior art. Additionally, the person of ordinary skill in the art would have readily realized that the terms biometrics is broadly used (i.e. inclusive of photograph/images) and recognize the use of templates as a digital photographic representation of a users biometric data.

As to the remarks regarding, a second party not needing to see his photograph, the examiner position is that it is the possessor of the biometric device (i.e. seller, merchant, owner, corporation etc.) that desires to authenticate the identity of another or client. Again, Appellant appears to have demonstrated a differences in wording not a patentable distinction between user, client, or party. Because, the term biometrics are known to encompass a wide range of devices, and since the term posses can not serve to distinguish, and further because, the use of photographic information was notoriously well known to persons of ordinary skill in the art as early as 1991; the examiner believes that the prior art of '236, '476, '204 and '156 all teach that the use of photographs was notoriously well known, and that their systems was capable of utilizing this biometric attribute. Notwithstanding, even appellant has recited in his disclosure that the use of

Art Unit: 2134

photographs as a biometric was well known, far in advance of his filing an application some 9 years later. Lastly, it is noted that the first party does nothing functional except possess the device, whether it is ownership or seizure of the device, it is not believed to be a patentable distinction.

As to claims 2,4,7,11,13 and 16 they stand or fall with claims 1 and 10 above, and are believed to be non-patentable for the reasons discussed above.

As to the remarks regarding claims 19-27, they recite method claims of the system and computer program product of claims 1-18, as such they repeat the claims and corresponding limitations in method format. The examiner grouped them together as a convenience, as they fails to recite any additional features that were not already previously recited and rejected. The examiner could have put the individual method claims with their corresponding product and apparatus or system claims; however, that would not have changed or added anything to the scope or metes and bounds of the rejected claims. Accordingly, the rationale for the rejected claims, product and system, similarly apply to these corresponding claims of the method. The examiner does not believe that this grouping has prejudiced or had an adverse effect on appellant in any way. The claimed subject matter has been identified for Appellant, in the office actions and rejections set forth by the Examiner. Additionally, an interview was given to appellant's representative further describing the examiner's interpretation and explanation. The differences in these interpretations are now the subject matter of this appeal, which is to be decided by the Board.

As per claims 5-6,8-9,14-15, and 17-27, appellant remarks that the examiner has not established prima facie obviousness for these claims; the examiner disagrees. The examiner has combined two references '326 and '476 to develop a 103 rejection. '236 states that an object of his invention is to provide an authenticating framework for use in authenticating clients having a plurality of authentication device types, and to enable client-server and internet based applications to use alternate authentication devices. Lastly, he recites that his framework provides the capability of managing authentication request traffic form a variety of clients having disparate devices and schemes/methods. (see '236 at col. 1, lines 60 thru col. 2, lines 24 et seq.). '476 recites that his invention is concerned with the portable information and transaction processing in PDAs (also referred to in '236 as a pervasive device). '476 goes further, to recite the that his invention will make use of biometrics, as a means for authenticating a client (col. 3, lines 45-50 et seq.). Therefore, the combined effect of using the two references as they are intended lends themselves to biometrically authenticating individuals, with a portable PDA/pervasive device, as recited in the office action. The various uses of a biometric device has also been referred to in both references ('236 column 1, 40 et seq., col. 3, lines 25 et seq., col. 4, lines 34 et seq., col. 5, lines 5-14, col. 6, line 15-20, and '476 col. 2, lines 24 et seq.). Therefore, it is believed by that there is sufficient motivation, and reason for modifications found in each reference to support the combination, for a 103 rejection.

Appellant also remarks that claims 8,17 and 26, limitations have not been taught, the examiner does not concur. These claims recite a product, system and

Art Unit: 2134

method (for example claim 8 recites) "...is used to enable on demand creation of a secure meeting site by repeating the operation of said means for capturing and ...means for identifying for each of a plurality of meeting attendees." The examiner broadly interprets this as, a means of repeatedly identifying and or authenticating (biometrically) members/people attending a meeting site. Please take note the following: 1. The device is not an integral part of the meeting site. 2. The device is not being used in any manner that is inconsistent with verifying users biometrically, as is known in the art. 3. The operation of the device is not affected by the fact that it is being utilized to authenticate and verify repeatedly, the identity of a plurality of attendees/ device users, whom are at a gathering. The claimed limitations of repeatedly identifying people with a device, who happened to be gathered for a meeting in a site, does not change the structure or operations of the authenticating device being used. This appears to be nonfunctional descriptive language, since it does not impart any functionality to the claims. In this instance, we see that the device would operate the same whether one person or different and successive people utilized the device to have their identity authenticated and verified. The limitation of securing a meeting place by verifying the attendees would have to be integrated into the device (structurally and/or functionally) for the terms 'securing a meeting site' to be given patentable weight. Here, we have people repeatedly using the device to verify their identity, access to the meeting site is only secured if someone keeps track of all the people entering and leaving who has been authenticated. It is parallel to asking to see someone's identification or badge at a meeting site; in the claimed invention, the person desiring to

Art Unit: 2134

be verified gives a biometric sample that is compared to a stored template image (somewhere) to verify and authenticate his identity. The fact that there is a gathering of individuals in a site is immaterial, as it is nonfunctional descriptive language that does not relate to nor does it affect the functionality and operations of the biometric pervasive device. As result, the non-functional descriptive language does not limit the claim and thus not can not serve to distinguish.

Assuming, that the examiner did give the limitation some patentable weight, then we have a claim that makes use of a biometric authentication device for verifying multiple people/attendees at a site. The fact that they are attendees at a meeting site would not further limit the claims for the reasons stated above, the site is not integral to the device and its operation. Thus, securing a meeting site appears to be non-functional descriptive language describing an intended use. The biometric identification and authentication of a plurality of users, is merely a device having access to a database or system that has more than one template for verifying a plurality or users. The number of users and the fact that they are in one place fails to change the structure of the device or cause the device to operate and function any differently than before.

However, the examiner attempted to show appellant that said use of biometric devices for the purpose of gaining access to a meeting site, building, room, gathering place etc., is well known to one of ordinary skill in the art; by reciting Maes et al., U.S. Patent Number 6,016,476, hereinafter, '476. In the final office, dated 6/1/2005, the 103 rejection of Crane '236 in view of Maes '476, whereby Maes '476 was has been grossly incorporated into Crane '236, the examiner recited a teaching from the prior art '476 that

Art Unit: 2134

clearly recites that biometric pervasive devices could be used for access control to a building. '476 recites "... another object of the present invention to provide a PDA [pervasive device] with digital certificate security which can be extended to all applications or systems wherein magnetic and/or smart cards are used such as access control cards for accessing a device service or building, ...employee cards for accessing confidential information." The invention of '476 uses similar language with regards to employees accessing a secure site/building. It is believed, that even if the examiner gave some patentable weight, to the attendees or employees or workers, gathering at a site or building for a work meeting; that said use would clearly fall within the scope a pervasive biometric device identifying the users for gaining access. The prior art of '476, filed many years before appellant, appears to supports such uses as recited in column 2, lines 53 et seq. This does not appear to be a new or non-obvious use for pervasive devices; it appears to be one of the well known-uses, as evidenced above.

As to the remarks, regarding claims 9, 18, and 27 exchanging a trusted message, by performing a biometric identification, this has been addressed. '476 at column 2, lines 31, teach that a user must be verified via biometrics prior to accessing and writing a digital certificate, selected financial and personal information into his PDA (on the card). It further recites, at column 2, lines 44 et seq.; digital data exchanges via a PDA (pervasive device) may be secured via biometric in an electronic data transfer. This is explained in more detail at column 3, lines 15-45. '476 also teach the use of encryption for secure message exchanges at col. 5, lines 10-25 et seq., following the

Art Unit: 2134

authentication of a user biometrically. '476 also utilizes his invention for other means of conveying trusted messages such as consumer transaction, see col. 7, lines 35 et seq. Therefore, the combination of '236 and '476 has been considered to explicitly teach the use of exchanging trusted messages.

Claims 21, is similarly believe to be unpatentable for the reason recited with regard to claims 3 and 12. As it is method of retrieving information which comprises a photograph, deemed digital template, or digital image or digital photographic information as is well-known in the art by skilled artisans.

All of the remarks by Appellant has are believed to have been addressed. This answer describes well-known uses for biometrics, such as access control, identification and authentication of users (second party or attendees), securing access to controlled sites (meetings), the use of retrieving digital photographic information (template or digital image data) representative of a persons physical attributes, as well as the electronic exchange of trusted messages – via PDAs, or pervasive, following prior biometric verification. These principals and techniques have been demonstrated in the prior art as evidenced in '236, and '476, as well as, Appellant's own specification and admitted prior art (page 2, 1st. para, and page 4, 2nd. Para.).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Art Unit: 2134

Respectfully submitted,


Norman M. Wright

AU 2134



NORMAN M. WRIGHT
PRIMARY EXAMINER

Conferees:

Gilberto Barron

 5/18/06

Matthew Smithers

 5/24/06